



Department of Homeland Security Daily Open Source Infrastructure Report for 20 April 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports a woman was hospitalized earlier this month with bubonic plague, the first confirmed human case in Los Angeles in more than two decades. (See item [24](#))
- Reuters reports hospital executives say they cannot do everything that is necessary to prepare for a possible bird flu outbreak, and that the U.S. and other countries have too few drugs, supplies, and equipment to deal with a respiratory virus pandemic. (See item [25](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *April 19, Christian Science Monitor* — **Should oldest U.S. nuke plant stay on line?** In what could be a precedent-setting case, New Jersey and a citizen coalition are fighting renewal of the license for the nation's oldest operating nuclear power plant. Their concern: The structural design of the 1960s-era Oyster Creek nuclear generating station is a security risk because, among other things, it stores highly radioactive spent fuel rods above ground, which could make it vulnerable in the event of a terrorist attack. Their contention, if proved, could lead the Nuclear Regulatory Commission (NRC) to deny for the first time a nuclear generating station's request for a license renewal after its original 40-year license expires. It could also set a new

standard for the NRC, which currently does not take terrorism into account when it decides whether to renew a nuclear plant's license. The NRC recently ruled the "possibility of a terrorist attack ... is speculative" and therefore "beyond the scope" of relicensing proceedings. The state of New Jersey is appealing, arguing that the threat of terrorism is not speculative but a danger that must be addressed. "From a policy perspective, it's absolutely critical that the relicensing procedures take into account the vulnerability from man-made attacks," says Michael Greenberger of the University of Maryland.

Source: <http://www.csmonitor.com/2006/0419/p03s03-ussc.html?s=hns>

2. *April 19, Associated Press* — **Snowstorm causes widespread power outages in northern Plains.** Up to two feet of blowing snow closed major highways on the northwestern Plains on Wednesday, April 19, as a powerful storm caused widespread power outages and was blamed for at least three deaths. More than 2,000 homes and businesses lost power in South Dakota's Black Hills, and many schools were closed. On Wednesday, the Mountrail-Williams County Electric Cooperative said that some towns in western North Dakota could be without electricity for another day. The heaviest snowfall was reported in the Black Hills, with 24 inches at Lead and Rochford, the National Weather Service said. Spring storms with heavy snow aren't unusual in North Dakota, said weather service meteorologist Jim Fors in Bismarck. "We don't get them every year, but every five to ten years, we usually get a big dump," Fors said.
Source: <http://edition.cnn.com/2006/WEATHER/04/19/spring.storms.ap/>
3. *April 19, Pittsburgh Post-Gazette* — **Truck trying to enter power plant has \$500,000 seized.** State police seized more than \$500,000 from a truck at the Beaver Valley power plant in Shippingport, PA, on Tuesday, April 18. Two men in a tractor trailer tried to enter the plant around 4:15 p.m. EDT to pick up large tool containers. During a routine inspection, plant security discovered a duffel bag with a large amount of cash. State police were called, but in the meantime, the truck left. Police stopped it a mile away and the driver said he didn't know anything about the money or who gave it to him. The duffel bag contained ten large bundles of cash, totaling \$504,230. The situation drew the support of the state police/FBI Joint Terrorism Task Force.
Source: <http://www.postgazette.com/pg/06109/683297-100.stm>
4. *April 18, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission proposes \$3,250 civil penalty against firm for loss of portable nuclear gauge.** The Nuclear Regulatory Commission (NRC) has proposed a \$3,250 fine against a San Juan, Puerto Rico-based company for violations associated with the loss of a portable nuclear gauge in August 2005. The gauge, which contains radioactive material, is used for industrial purposes such as measuring soil density. On August 16, 2005, an employee of GEO-EXPLOR, Inc., was using the gauge at a temporary job site in Dorado, Puerto Rico. Upon completion of work, the employee placed the device in the open bed of a pickup truck but failed to secure it to the vehicle or to close the tailgate. The gauge fell off the truck after traveling a distance. The gauge was subsequently recovered — intact and undamaged — by a member of the public. NRC Region I Administrator Samuel J. Collins wrote: "...these violations are of concern to the NRC because (1) the gauge was in the public domain for approximately 6 days, and (2) such sources can result in unintended radiation exposure to an individual if the (radioactive) source is not in the shielded position."

Source: <http://www.nrc.gov/reading-rm/doc-collections/news/2006/06-025i.html>

5. *April 18, New York Times* — **Chemical companies look to coal as an oil substitute.** With oil and natural gas prices showing no signs of plummeting, and with incentives to use coal built into the Energy Policy Act of 2005, coal could become a common substitute for oil. Chemical companies, which use oil and gas as feedstocks, are hoping it will happen soon. "We want to be economically feasible in the U.S., and coal enables us to do that," said Andrew N. Liveris, chief executive of Dow Chemical, which has tripled its research into coal-based ingredients. According to the American Chemistry Council, the industry's cost for feedstocks hit \$40.12 billion last year, up from \$34 billion in 2004, \$25.1 billion in 2003 — and triple the \$12.8 billion in 1999. Several Chinese companies already use coal to make vinyl chloride monomer, a precursor to the polyvinyl chloride used to make construction products like pipes. Andrew Wood, the editor of Chemical Week magazine, said that numerous American and European companies would open plants in China to make other chemicals from coal, too. Manufacturers are preparing themselves for an onslaught of orders for coal gasification equipment. Source: <http://www.nytimes.com/2006/04/18/business/18chem.html?ei=5087%0A&en=e53448814ddacf81&ex=1145505600&pagewanted=print>

6. *April 17, Associated Press* — **Venezuela oil refinery still down.** A Venezuelan oil workers' union said Monday, April 17, that the country's 300,000 barrel-a-day Cardon oil refinery is still not producing gasoline — a key export — after a power outage idled the facility last week. State oil company Petroleos de Venezuela said Sunday, April 16, it had partially restored production to 200,000 barrels a day after an electrical fault forced it to shutdown operations early Friday, April 14. But Francisco Garcia of the Sinutrapetrol oil union said the refinery still was not producing gasoline because key processing units remained down, adding that there was an explosion on Sunday, April 16, at the refinery's reformer unit, which produces reformulated gasoline. The Cardon complex has been plagued by accidents over the past year, including at least three outages and a series of fatalities. Venezuela is the world's fifth-largest oil exporter and a top supplier to the U.S. Source: http://biz.yahoo.com/ap/060417/venezuela_refinery.html?v=1

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

7. *April 19, Villages Daily Sun (FL)* — **Ruptured gas line forces evacuation of homes.** Construction workers punctured a main natural gas line Tuesday, April 18, prompting firefighters to evacuate four Village of Winifred, FL, homes. A crew working for C and N Foundation Technologies struck the 2-inch line while digging beneath a home in order to fill a depression in the earth with concrete. Gas could be heard rushing from the line as firefighters blocked off an area approximately 150 feet around and made sure nearby residents were out of their homes. Source: <http://www.thevillagesdailysun.com/articles/2006/04/19/villages/villages01.txt>

[[Return to top](#)]

Defense Industrial Base Sector

8. *April 19, National Defense* — **Air Force: Preparing to award \$500 million contract for training.** The Air Force is preparing to award a contract worth as much as \$500 million over the next five years to provide training for its combat search and rescue personnel. The job — dubbed aircrew training and rehearsal support II, or ATARS II — essentially will be a follow on to a \$277-million, six-year award originally won in 2000 by Lockheed Martin Information Systems, of Orlando, FL, said program manager Greg Riddle, in the Ogden Air Logistics Center at Hill Air Force Base, UT. The service plans to award the contract in August or September, with the work to start in January 2007, Riddle said. The winner will provide mission-qualification training and mission-rehearsal system hardware, software and courseware, including instructors, for Air Force special operations units at Kirtland Air Force Base, NM; Hurlburt Field, FL; and Harrisburg, PA. The training will cover the MH53J/M Pave Low, UH-1N Huey and HH-60G Pave Hawk helicopters; the CV-22 Osprey tilt-rotor aircraft, and several special-operations versions of the C-130 Hercules fixed-wing transport.
Source: <http://www.nationaldefensemagazine.org/issues/2006/May/RaceBegins.htm>

[\[Return to top\]](#)

Banking and Finance Sector

9. *April 18, Top Tech News* — **Phishing steals spotlight at MIT spam conference.** Phishing is destroying banks' and other companies' ability to communicate with their customers in the most effective way, said Paul Judge of CipherTrust. "Some of the most powerful entities on earth can't talk to their customers over e-mail" because phishing has corroded their customers' trust, he said. While the volume of unwanted e-mail ebbs and flows, the nature of unwanted e-mail is steadily becoming more dangerous, say spam experts at the MIT Spam Conference held in Cambridge, MA, recently. No technology has been developed that can effectively protect e-mail users from phishing attacks that steal personal and financial information, and until this form of fraud can be detected and blocked, unwanted e-mail remains a threat. "The spam problem will get worse, and the reason is phishing," said Bill Yerazunis of Mitsubishi Electric Research Laboratories. Yerazunis estimates 20 to 30 percent of all spam messages are phishing attacks. The response rate for phishing e-mails is higher than for spam, said Judge of CipherTrust. So while spammers have to send more unsolicited e-mail, as antis spam filters get better at identifying and blocking spam, phishing attacks are well enough disguised that a higher percentage of recipients click on them, he said.
Source: http://www.toptechnews.com/story.xhtml?story_id=10200002LMVO

[\[Return to top\]](#)

Transportation and Border Security Sector

10. *May 01, National Defense* — **Lawmakers introduce tunnel legislation.** The movement of illegal immigrants or narcotics through a tunnel under a U.S. border is a felony, but there are no laws on the books preventing the excavation itself. Bipartisan legislation aiming to close this loophole has been introduced in both houses of Congress. Eight tunnels have been discovered in the San Diego area since the beginning of this year. Forty have been found so far, with 39

along the southern border and one under the northern border. Some are simple “gopher holes,” only a few feet long near a fence. Others are sophisticated, well-engineered constructions replete with lights, pulleys, drainage and ventilation systems, and well-hidden entrances. The bills will make it a federal violation to build or finance a tunnel. Judges could hand down sentences of up to 20 years. Those who “recklessly” allow a tunnel to be built on their property may face up to 10 years. The proposed law would also double sentences for those who use tunnels to smuggle aliens, contraband or terrorists. Meanwhile, efforts continue to improve tunnel detection. Joint Task Force North, out of Fort Bliss, TX, has a unit dedicated to applying technologies used in the civilian sector for mining and other geological applications to the esoteric field of detecting underground passageways.

Source: <http://www.nationaldefensemagazine.org/issues/2006/May/Lawmakers.htm>

11. *April 19, USA TODAY* — **Rising jet fuel costs may push airline tickets up.** The millions who are expected to make this summer's air travel season the busiest ever should soon begin feeling the pain of the 24 percent run-up in crude oil prices since February 15. Jet fuel closed Tuesday, April 18, at \$90.30 a barrel on the Gulf Coast spot market, which is the highest price ever, excluding the weeks immediately following Hurricane Katrina. Peter Belobaba, principal research scientist at MIT's Center for Transportation and Logistics, says airlines are likely to pass through their higher costs. Belobaba says travelers might see the effects in three ways: fewer seats in the lowest-price categories, big increases in business fares, and somewhat smaller increases in leisure fares. Belobaba says, "It could well make sense to get \$10 or \$20 more from the large proportion of (passengers) paying the lowest fares (vacationers) than to try to get \$50 or \$100 more from the small number of high-fare business travelers." Until recently, fares had been at or near historically low levels for several years.

Source: <http://www.usatoday.com/travel/flights/2006-04-18-jet-fuel-ux.htm>

12. *April 19, USA TODAY* — **Airports leery on traveler registry.** Only one of the U.S.'s busiest airports has signed up for a program to speed travelers through checkpoints, while at least a half-dozen others are balking at an idea that they say won't work. The lack of sign-ups could threaten the Registered Traveler program, pushed by Congress for years as a way to speed up post-9/11 security lines by giving minimal inspections to air travelers who pass a background check. A lack of support raises the prospect that the program may not become a nationwide network that gives participants a quick pass through security. Four major airports have already said no, four more say they are skeptical and a dozen others are undecided even as the program prepares for its debut. The Transportation Security Administration plans to start approving Registered Traveler programs at airports on June 20 at a time when airports fear long security lines will delay summer travelers. But so far only one of the nation's top 20 airports, Orlando, has signed up and hired a company to run its program.

Source: <http://www.usatoday.com/travel/flights/2006-04-18-airport-registry.htm>

13. *April 19, Aero-News Network* — **Washington State DOT antes up \$13.3 million for airport improvements.** Declaring that "we are committed to preserving the state's aviation system by stretching our state grant funds to the maximum extent," Washington Aviation Operations Manager Stan Allison announced Wednesday, April 19, the state's Local Airport Aid Grant Program has appropriated \$13.3 million for 39 different airport improvement projects throughout the state. A total of 31 public-use airports in Washington will benefit from Washington State Department of Transportation's (WSDOT) latest round of state, local and

federal grants awarded during the 2005–2007 biennium. Of the total \$13.3 million awarded, WSDOT used approximately \$1.8 million in state grants to fund the projects. WSDOT reports airport improvement projects slated for the 2005–2007 biennium are in the areas of pavement, safety, planning, maintenance, security, and runway safety. Pavement maintenance — the main focus of WSDOT’s grant program — understandable, given the effect Washington’s rainy weather has on concrete and asphalt — comprises about 78 percent of the planned projects.

Further information: <http://www.wsdot.wa.gov/aviation/>

Source: <http://www.aero-news.net/index.cfm?ContentBlockID=a53dc5f1-203f-4e61-be47-1b74bfe35cfe>

- 14. *April 19, Associated Press* — Suspicious device found at Atlanta airport.** Hartsfield–Jackson Atlanta International Airport officials closed down all security checkpoints for about two hours Wednesday afternoon, April 19, after a "suspicious device" was detected in a screening machine. The gates were reopened shortly before 4 p.m. EDT. By that point, there had been no departures for more than an hour, and all arriving flights were delayed at least 90 minutes, according to the Federal Aviation Administration’s Kathleen Bergen. She said this is peak travel time and at least 120 flights had been affected. After the gates were reopened, hundreds of passengers waited in a line stretching from the airport’s baggage claim area to the main atrium. The airport remained open and operating throughout the afternoon, although airport spokesperson Felicia Browder acknowledged there was no way for passengers entering the airport to get to their airplanes. Browder said an airport explosive detection unit was deployed.

Source: http://www.usatoday.com/travel/flights/2006-04-19-atlanta-security-alert_x.htm

[[Return to top](#)]

Postal and Shipping Sector

- 15. *April 19, Federal Times* — Day: Other agencies unprepared for anthrax threat.** Some agencies still have not developed procedures for handling an anthrax attack, the threat of which “remains credible,” says Tom Day, the U.S. Postal Service senior vice president of government relations. Day said, “The U.S. mail is clearly safer than what other [deliverers] are doing. . . . If there is a risk, it may be greatest with independent delivery services. Agencies need to look at all correspondence and packages.” Last year the Postal Service completed the deployment of biodetection apparatus at all 1,086 automated mail processing centers in the country, Day said. At a General Services Administration forum last month, Day outlined five components that each agency’s anthrax plan must have. They are an analysis of credible threats, an awareness of all delivery and courier activity, an understanding of detection technology they are using, a protocol for sampling a suspect material, and a good response plan. The Postal Service will now concentrate some of its attention on reducing the cost of its anthrax detection program, which runs about \$120 million each year.

Source: <http://federaltimes.com/index.php?S=1688151>

[[Return to top](#)]

Agriculture Sector

16. *April 19, Associated Press* — Japan confirms twenty-fifth case of mad cow disease. Japan has confirmed its 25th case of mad cow disease in a five-year-old Holstein, officials said Wednesday, April 19. Meat inspectors in Okayama Prefecture found late Monday that a dairy cow, intended to be slaughtered for meat, had tested positive for the disease. A panel of Health Ministry experts confirmed the infection Wednesday, according to ministry official Kenichi Watanabe.

Source: http://mdn.mainichi-msn.co.jp/business/news/20060419p2g00m0b_u038000c.html

17. *April 18, Animal and Plant Health Inspection Service* — New Jersey trees to be treated against Asian longhorned beetle. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) will treat 27,589 trees susceptible to the Asian longhorned beetle (ALB) in New Jersey this spring, including approximately 4,800 trees to be added to the ALB quarantine as a result of an infested tree recently discovered in Linden, NJ. These treatments are part of the ALB cooperative eradication program's effort to prevent further infestation of this invasive insect pest and reduce beetle populations. APHIS will treat trees in portions of the established 20-square mile quarantine area in New Jersey with the insecticide imidacloprid, which has yielded positive results in past treatments. Program officials will treat 12,279 trees in Linden, 6,557 trees in Woodbridge, 4,647 trees in Carteret, 3,585 trees in Rahway and 521 trees in Roselle. The 4,800 additional trees to be treated this year are in Linden and Roselle, NJ. Tree treatments began April 17 and will last until the middle of June. ALB information: <http://www.uvm.edu/albeetle/>

Source: http://www.aphis.usda.gov/newsroom/content/2006/04/albnj06_p pq.shtml

18. *April 18, Xinhua (China)* — Foot-and-mouth disease hits over 2,500 animals in Vietnam. Up to 2,550 pigs and bulls in Vietnam's central highlands Lam Dong province have been infected with foot-and-mouth disease in recent days, local newspaper Pioneer reported Tuesday, April 18. The disease has hit the pigs and bulls in seven out of 12 districts and towns in the province. Most of the infected animals are in Duc Trong district. By Monday, 2,250 animals in the district contracted the disease, more than 800 of them died.

Source: http://english.people.com.cn/200604/18/eng20060418_259235.ht ml

[\[Return to top\]](#)

Food Sector

19. *April 18, Food Safety and Inspection Service* — Chicken toddler food recalled. Beech-Nut Nutrition Corporation, a Canajoharie, NY, firm, is voluntarily recalling approximately 9,465 pounds of chicken product due to the possible presence of pieces of bone, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, April 18. The chicken product was produced on January 3, 2006, January 26, 2006, March 20, 2006 and March 21, 2006, and was distributed to retail stores nationwide. The problem was discovered by the company. FSIS and the company have received no reports of injury from consumption of this product.

Source: http://www.fsis.usda.gov/News_ & Events/Recall_013_2006_Relea se/index.asp

[\[Return to top\]](#)

Water Sector

20. *April 18, Lawrence Journal–World (KS)* — **Summer forecast includes little water.** A dire weather forecast issued Monday, April 17 calls for a hot, dry summer across the Kansas Plains reminiscent of the 1930s — the era of the devastating Dust Bowl drought. The Pennsylvania–based forecasting service AccuWeather.com predicts a high–pressure system will be parked across the central U.S. much of the summer that would lead to scorching–hot days and prevent moisture from coming into the region — something that in turn causes even higher temperatures.
Source: http://www2.ljworld.com/news/2006/apr/18/summer_forecast_doe_snt_hold_water/
21. *April 18, Associated Press* — **State water board approves plan for two new reservoirs.** The Texas Water Development Board on Tuesday, April 18 approved a long–range regional plan that includes building two reservoirs in Northeast Texas and pumping the water hundreds of miles to the Dallas–Fort Worth area. The regional water plans are designed to help the state meet the water needs of the next 50 years when the population could nearly double to more than 40 million. The plan includes the construction of the \$2.1 billion Marvin Nichols Dam on the Sulphur River and the \$569 million Fastrill Dam on the Neches River.
Source: <http://www.chron.com/dispatch/story.mpl/metropolitan/3803050.htm>

[[Return to top](#)]

Public Health Sector

22. *April 19, Associated Press* — **Mumps cases jump by more than 200 since last week.** The number of mumps cases in Iowa jumped by more than 200 in the past week, with state health officials saying the rise is a combination of new cases and a logjam of paperwork from cases yet to be tallied. Kevin Teale, a spokesperson for the Iowa Department of Public Health, said Tuesday, April 18, that 210 cases of mumps have been reported since Thursday, April 13, bringing the total to 815. Officials have had the most trouble processing paperwork in Dubuque County, which has reported the most cases statewide. Mumps cases in Dubuque jumped to 323 from 187 in the past week, an increase Teale credits largely to backlogged cases that workers finally processed in the past five days. The disease also is being reported in more counties. As of Tuesday, 67 counties had reported mumps cases, up from 60 last week.
Mumps information: http://www.cdc.gov/ncidod/diseases/submenus/sub_mumps.htm
Source: http://www.wcfcourier.com/articles/2006/04/19/news/breaking_news/doc4445fcb04f62f915327690.txt
23. *April 19, Agence France–Presse* — **Anti–viral stockpile completed for World Health Organization.** The Swiss pharmaceutical company Roche says it has finished building a stockpile of three million courses of the antiviral drug Tamiflu for the World Health Organization (WHO). The so–called "Rapid Response Stockpile", which had been in the pipeline since Roche and the WHO signed a deal last August, was now ready to be shipped to the site of a major influenza outbreak, the group said in a statement on Wednesday, April 19. Tamiflu is considered a frontline drug against a potential human flu pandemic sparked by avian influenza.

Source: http://news.yahoo.com/s/afp/20060419/hl_afp/healthflupharma_060419094713

24. *April 18, Associated Press* — **Woman hospitalized with bubonic plague.** A woman was hospitalized earlier this month with bubonic plague, the first confirmed human case in Los Angeles, CA, in more than two decades, health officials said Tuesday, April 18. The woman was admitted April 13 with a fever, swollen lymph nodes and other symptoms. A blood test confirmed she had contracted the bacterial disease. The woman was placed on antibiotics and is in stable condition, officials said. Bubonic plague is not contagious, but if left untreated it can morph into pneumonic plague, which can be spread from person to person. Bubonic plague is usually transmitted to humans from the bites of fleas infected by dead rodents. Health officials suspect the woman was exposed to fleas in her central Los Angeles home.

Plague information: <http://www.bt.cdc.gov/agent/plague/>

Source: <http://www.breitbart.com/news/2006/04/18/D8H2OUH87.html>

25. *April 18, Reuters* — **We can't afford bird flu plans, hospital heads say.** The U.S. government may be urging local officials and hospitals to get ready for a bird flu pandemic, but top hospital executives said on Tuesday, April 18, they cannot do everything that is being called for. Experts say the U.S. and other countries have too few drugs, supplies such as latex gloves, or even equipment such as ventilators to deal with a pandemic of a respiratory virus. Preparedness could come down to more than having the medical equipment. "We may not have the staff needed to run those ventilators adequately," said Vicki Running, who heads disaster planning at Stanford University Medical Center in California. Day-to-day business is already overwhelming hospitals, according to Running. "We are operating at capacity," she said. Edward Miller, chief executive officer of Johns Hopkins Medicine, said the Baltimore hospital and medical school had already spent \$10 million preparing for a pandemic or other emergency. "This is not a sustainable business plan," Miller said. "I don't think anybody is capable of paying the entire price tag," agreed Thomas Burke, executive vice president of the M.D. Anderson Cancer Center in Houston. "There are none of us who can afford to absorb those kinds of costs."

Source: <http://today.reuters.com/news/articlenews.aspx?type=domestic>

[News&storyid=2006-04-18T230714Z_01_N184659_RTRUKOC_0_US-BIRD-FLU-HOSPITALS.xml](http://today.reuters.com/news/articlenews.aspx?type=domestic&storyid=2006-04-18T230714Z_01_N184659_RTRUKOC_0_US-BIRD-FLU-HOSPITALS.xml)

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

26. *April 19, Contra Costa Times (CA)* — **San Francisco hosts 100th Anniversary Earthquake Conference.** Get ready. That's the message Governor Arnold Schwarzenegger put across Tuesday, April 18, at the 100th Anniversary Earthquake Conference at San Francisco's Moscone Center commemorating the 1906 earthquake. The governor announced plans to beef

up California's ability to respond to disasters, including the creation of a new state Department of Public Health. The new department would be created by splitting the California Department of Health Services into two departments — one that would deal with individual health care concerns, and a new Department of Public Health that would take on emergency preparedness, drinking water, food and drug safety, and chronic and communicable disease. The governor also issued an executive order for the Office of Emergency Services to reach agreements with key vendors to get resources when and where they are needed in the aftermath of a disaster. "Managing Risk in Earthquake County" document prepared for the 100th Anniversary Conference: <http://1906eqconf.org/mediadocs/managingrisk.pdf>
 "When the 'Big One' Strikes Again" which presents interim results of an on-going study of building damage and losses likely to occur due to a repeat of the 1906 earthquake: <http://1906eqconf.org/mediadocs/BigonestrikesReport.pdf>
 Source: <http://www.contracostatimes.com/mld/cctimes/news/state/14376008.htm>

27. *April 18, GovExec* — **Acting FEMA chief backs suggestions for improved disaster response.** The Federal Emergency Management Agency's (FEMA) acting director, R. David Paulison, on Tuesday, April 18, said he supports recent recommendations from the Department of Homeland Security's (DHS) inspector general (IG) on strengthening disaster response, but added that the agency is several years away from completing all the necessary changes. "We're taking all reports with open arms," Paulison said, referring to the IG report and to other post-Hurricane Katrina reviews. He said he has flipped through the recommendations, and acknowledged the agency needs retooling. The report, issued Friday, April 14, called for revamped and improved information sharing among FEMA workers, and between the agency and the rest of DHS, state emergency responders and the public.
 Source: http://www.govexec.com/story_page.cfm?articleid=33868&dcn=to_daysnews
28. *April 18, Oregonian* — **Federal study: Oregon's emergency medical services system has undergone dramatic deterioration.** Oregon's emergency medical services (EMS) system, which licenses ambulance services and emergency medical technicians and oversees hospital trauma centers, was once so good it could have been a model for the nation. But things have decayed badly. A federal study released Monday, April 17, found that the state's EMS system has undergone such "dramatic deterioration" that it places Oregon residents at risk, and it called for "immediate, dramatic change." The main finding: Care of accident victims varies widely from place-to-place in Oregon. The National Highway Traffic Safety Administration performed the study at the request of the Oregon Department of Human Services. Among other things, surveyors criticized several elements of the state's program, saying: It lacks a medical director who can develop standards for all Oregon communities. Without standards it is impossible to measure how well services are delivered. Resources for emergency services vary widely across the state from urban to rural areas. And the report states that Oregon lacks a plan to improve services in frontier and rural areas.
 Source: http://www.oregonlive.com/news/oregonian/index.ssf?/base/fro nt_page/1145328928159390.xml&coll=7
29. *April 18, CBS 4 Denver* — **Colorado city tests residents' preparedness for flooding.** In an effort to raise awareness and preparedness for floods, the city of Boulder, CO, held their annual flood drill Tuesday morning, April 18. This year, the drill focused on a large-scale event that simulated what would happen if the Boulder Creek and parts of downtown flooded. Crews

sounded warnings sirens and did a mock evacuation of the affected areas and the residents' evacuation plan. The drill also helped emergency responders form a command center to respond to catastrophe.

Source: http://cbs4denver.com/topstories/local_story_108184457.html

30. *April 18, Stanford Daily (CA)* — **Stanford University: Prepared for disaster.** Stanford University, CA, officials say they are confident in their emergency planning, and that they take every precaution to prepare for a range of disasters, including earthquakes. An elaborate, publicly-available emergency plan details the response mechanism that would be put in place after an earthquake. A central operation center located at the Faculty Club would be activated by the incident commander and 26 satellite operation centers would come online. Each satellite center has developed its own local plan for what to do in the event of an earthquake. A contingent of volunteers on campus has agreed to look at buildings' exteriors to get a preliminary view of the damage. They will report back to the satellite command centers, helping engineers determine which buildings should be focused on immediately. The university emergency preparedness system is designed around an all-hazards approach, meaning that the protocol for an earthquake response is very similar to that of a terrorist attack. In addition, satellite phones have been procured so leaders on campus can maintain contact with others in the event of local outages. If all else fails, emergency planners have designed a system for runners to carry messages from satellite command posts to emergency headquarters.

For the complete text of the university's emergency plan:

<http://www.stanford.edu/dept/EHS/prod/general/erprep/plans/index.html>

Source: http://daily.stanford.edu/tempo?page=content&id=20093&repository=0001_article

31. *April 18, Baltimore Sun* — **Maryland warned of storm threat at conference.** After last year's devastating storms, including more than 1,300 deaths from Hurricane Katrina, the federal government's top hurricane forecaster came to Maryland's annual severe-storm awareness conference in Laurel Monday, April 17, to deliver one message: "If you think it will never be that bad again, I'm here to convince you otherwise." The federal government will not release its predictions for the 2006 hurricane season until next month. However, well-known hurricane forecaster William M. Gray of Colorado State University found a 64 percent chance that a major hurricane — Category 3 or larger — will hit the East Coast this year. The government will use two new strategies this hurricane season, which begins June 1. The Federal Emergency Management Agency is in the process of assigning disaster coordinators to 13 states, including Maryland. Also, the National Hurricane Center will release new information on the intensity of storms. The Air Force's hurricane hunter aircraft will carry instruments that measure foam on waves, a sign of wind strength. That data will be converted into a chart showing the probability of hurricane-force winds hitting an area.

Source: <http://www.baltimoresun.com/news/weather/hurricane/bal-fema0418.0,1459201.story?track=rss>

[[Return to top](#)]

Information Technology and Telecommunications Sector

32. *April 19, U.S. Computer Emergency Readiness Team* — **US-CERT Technical Cyber Security Alert TA06-109A: Oracle products contain multiple vulnerabilities.** Oracle

products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial-of-service. Systems affected: Oracle Database 10g; Oracle9i Database; Oracle8i Database; Oracle Enterprise Manager 10g Grid Control; Oracle Application Server 10g; Oracle Collaboration Suite 10g; Oracle9i Collaboration Suite; Oracle E-Business Suite Release 11i; Oracle E-Business Suite Release 11.0; Oracle Pharmaceutical Applications; JD Edwards EnterpriseOne, OneWorld Tools; Oracle PeopleSoft Enterprise Tools; Oracle Workflow; Oracle Developer Suite 6i. For more information regarding affected product versions, refer to the Oracle Critical Patch Update — April 2006.

Solution: Apply the appropriate patches or upgrade as specified in the Oracle Critical Patch Update — April 2006: <http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html>

Note that this Critical Patch Update only lists newly corrected issues. Updates to patches for previously known issues are not listed.

Source: <http://www.uscert.gov/cas/techalerts/TA06-109A.html>

- 33. April 18, FrSIRT — Apple Mac OS X security update fixes J2SE security bypass vulnerabilities.** Apple has released security updates to address multiple vulnerabilities identified in J2SE. These flaws could be exploited by malicious Websites to compromise a vulnerable system. Analysis: A security vulnerability in Java Web Start may allow an untrusted application to elevate its privileges. Due to an issue handling input method events, it is possible that key events intended for a secure field such as a password field may be sent to a normal text field in the same window. This could result in accidental password disclosure to others present when the password is entered. Affected products: Apple Mac OS X version 10.4.5; Apple Mac OS X Server version 10.4.5.

Solution: Upgrade to J2SE 5.0 Release 4 (Intel):

<http://www.apple.com/support/downloads/j2se50release4intel.html>

Or J2SE 5.0 Release 4 (PPC): <http://www.apple.com/support/downloads/j2se50release4ppc.html>

Source: <http://www.frsirt.com/english/advisories/2006/1398>

- 34. April 18, Secunia — Symantec LiveUpdate for Macintosh privilege escalation.** A vulnerability has been reported in Symantec LiveUpdate for Macintosh, which can be exploited by malicious, local users to gain escalated privileges. Analysis: The vulnerability is caused due to certain components not setting their execution path environment, which can be exploited to execute arbitrary programs with System Administrative privileges. Affected software: Symantec LiveUpdate for Macintosh 3.x; Symantec Norton AntiVirus for Macintosh 10.x; Symantec Norton AntiVirus for Macintosh 9.x; Symantec Norton Internet Security for Macintosh 3.x; Symantec Norton Personal Firewall for Macintosh 3.x; Symantec Norton SystemWorks for Macintosh 3.x; Symantec Norton Utilities for Macintosh 8.x.

Solution: Apply latest LiveUpdate patch.

Source: <http://secunia.com/advisories/19682/>

- 35. April 18, IT-Observer — Hackers sneak through browser vulnerability.** Security experts from MicroWorld Technologies claim that a new exploit, named "Exploit.JS.CVE-2006-1359.c," is used by hackers to sneak into computers through a vulnerability in Internet Explorer (IE). Exploit.JS works by pushing an unexpected and

unrecognizable HTML element that crashes IE. Then the Exploit forces IE to execute a malicious program to infiltrate into the computer. The vulnerability stems out from the way in which IE displays Webpages that use unexpected methods to call some HTML objects.

Microsoft has already identified this loophole and has released a patch.

Source: http://www.it-observer.com/news/6119/hackers_sneak_through_browser_vulnerability/

36. *April 18, SophosLabs* — **First spammer found guilty under Australian Spam Act.** The Australian Communications and Media Authority has successfully prosecuted its first spammer under Australia's Spam Act laws. The Perth, Western Australia-based spammer, Wayne Mansfield, and his company Clarity1, were found to have illegally sent more than 56 million spam messages in the 12 months since the act was introduced in April 2004.

Source: http://www.sophos.com/pressoffice/news/articles/2006/04/ozsp_am.html

37. *April 18, U.S. Navy* — **National Security Agency sponsors Cyber Defense Exercise.** The U.S. Naval Academy joined forces with fellow service academies in the sixth annual Cyber Defense Exercise (CDX) held Monday–Friday, April 10–14, at the Academy in Annapolis, MD. Sponsored by the National Security Agency, CDX brings Midshipmen and their peers together to create a computer network they must then defend against attack from hackers. The service academy that best defends its portion of the network from attack wins the competition. Results will be announced between late April and early May. The hackers in the exercise tested the security of the network, observed how long it took the students to become aware of the attacks, and assessed how they responded.

Source: http://www.news.navy.mil/search/display.asp?story_id=23208

38. *April 17, Air Force Link* — **New radio technology keeps troops in touch.** Riding as part of a convoy escort team outside the wire, the airman feels alone. Feeling nervous, he keys his radio microphone to check in with his base — and hears nothing but dead air. To ensure scenarios like this don't occur, the Air Force is leading a joint implementation of a new "Radio over Internet Protocol Routed network" communication system, known as the RIPRnet. "With the RIPRnet we have tied convoy radios in with Internet-based technology to extend their range," said Colonel Greg Touhill, U.S. Central Command Air Forces–Forward communications director at the Combined Air Operations Center. "This system provides more reliable and robust communications for our soldiers, sailors, airmen and marines who are out on the roads of Iraq." Better communications could make the difference between life and death for troops in Iraq, but that is not the only benefit of the RIPRnet. Other applications include use for air defense and command and control of close-air-support missions.

Source: <http://www.af.mil/news/story.asp?id=123019140>

Internet Alert Dashboard

DHS/US–CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US_CERT Operations Center Synopsis: US-CERT is aware of an active exploitation of a cross site scripting vulnerability in the eBay website. Successful exploitation may allow an attacker to take various actions, including the following:

Obtain sensitive data from stored cookies
Redirect auction viewers to phishing sites where further disclosure of login credentials or personal information can occur
Create auctions that use script to place login areas on the eBay website, where credentials may be sent to a remote server with malicious intent

For more information please review the following advisory and vulnerability notes:

CA-2000-02 – Malicious HTML Tags Embedded in Client Web Requests.

<http://www.cert.org/advisories/CA-2000-02.html>

VU#808921 – eBay contains a cross-site scripting vulnerability.

<http://www.kb.cert.org/vuls/id/808921>

US-CERT recommends the following:

Securing Your Web Browser

http://www.us-cert.gov/reading_room/securing_browser/#how_to_secure

Malicious Web Scripts FAQ

http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

eBay Spoof Email Tutorial

http://pages.ebay.com/education/spoof/tutorial/spoof_3.html

US-CERT Cyber Security Tip ST04-014.

<http://www.us-cert.gov/cas/tips/ST04-014.html>

Cyber Security Tip ST05-010. <http://www.us-cert.gov/cas/tips/ST05-010.html>

Add "ebay.com" to the Restricted Sites zone in Internet Explorer.

Phishing Scams

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	6881 (bittorrent), 32768 (HackersParadise), 41170 (---), 1026 (win-rpc), 113 (auth), 80 (www), 135 (epmap), 445 (microsoft-ds), 25 (smtp), 139 (netbios-ssn) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

